UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/668,046	09/22/2003	Oscar V. Zhuk	08223/100S137-US3	7300

7278   7590   02/25/2009
DARBY & DARBY P.C.
P.O. BOX 770
Church Street Station
New York, NY 10008-0770

EXAMINER
HO, VIRGINIA T

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
02/25/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _22 September 2003_.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-22_ is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) _1-5, 11-15, 20-22_ is/are rejected.
7)☒ Claim(s) _5-10,13 and 16-19_ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on _22 September 2003_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _See Continuation Sheet_.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :07/26/2004, 06/04/2007, 09/26/2007, 10/26/2007.

DETAILED ACTION

1.   The instant application having Application No. 10/668,046 filed on September 22, 2003

is presented for examination by the examiner.

Claim Objections

2.   Claim 13 is objected to because of the following informalities: *inconsistent terminology.*

The limitation recites a "computing process," which was previously referred to as a "client

process."

       Appropriate correction is required.

3.   Where applicant acts as his or her own lexicographer to specifically define a term of a

claim contrary to its ordinary meaning, the written description must clearly redefine the claim

term and set forth the uncommon definition so as to put one reasonably skilled in the art on

notice that the applicant intended to so redefine that claim term. *Process Control Corp. v.*

HydReclaim Corp., 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The term

"*consequence*" in claim 5 is used by the claim to mean "*consecutive data for a sequence*", while

the accepted meaning is "*something produced by a cause or necessarily following from a set of*

conditions." *(Merriam-Webster)* The term is indefinite because the specification does not clearly

redefine the term.

Claim Rejections - 35 USC § 102

4.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on
> sale in this country, more than one year prior to the date of application for patent in the United States.

6.   Claims 1-5, 11-15, and 20-22 are rejected under 35 U.S.C. 102(b) as being anticipated by

"Intrusion detection using sequences of system calls", Hofmeyr, et al. *(hereinafter Hofmeyr)*.

As per claims 1, Hofmeyr teaches a method and apparatus for verifying integrity of a

computing process, comprising: determining a trait associated with the computing process *(page*

152, system calls serve as the observable characteristic of a program); determining a pattern

statistic associated with the trait based in part on an execution of the computing process in a

normal condition *(page 153, data is collected of normal behavior in a normal execution*

environment); determining a prototype statistic associated with the trait based in part on another

execution of the computing process in another condition *(page 158, new traces of behavior are*

collected, using the same method as for collecting a pattern of normal behavior); comparing the

pattern statistic to the prototype statistic *(page 155, deviations from normal behavior may*

indicate possible intrusions. Hence, behavior at another instance is compared against normal

behavior to determine any deviations.); and if the comparison indicates abnormal behavior the

computing process, performing a predetermined action *(page 155, the IDS informs the system*

administrators of anomalous or intrusive behavior).

As per claim 2 and 13, incorporating the rejections of claims 1 and 11 (respectively),

Hofmeyr additionally teaches the method and apparatus wherein performing the predetermined

action further comprises performing at least one of sending an alert message *(page 155, the IDS*

informs the system administrators of anomalous or intrusive behavior), and disabling the

computing process.

As per claims 3 and 14, incorporating the rejections of claims 1 and 11 (respectively), Hofmeyr additionally teaches the method and apparatus wherein the trait further comprises at least one system level call *(page 153, irregularities in the behavior of programs are detected by observing system calls)*.

As per claim 4, Hofmeyr teaches the method of claim 1 as applied above. Hofmeyr additionally teaches the method wherein determining the pattern statistic and the prototype statistic further comprises: determining a trend associated with the trait during execution of the computing process in the normal condition *(page 177, normal behavior is defined in terms of short sequences of system calls executed by running privileged processes)*; and determining another trend associated with the trait during the other execution of the computing process in the other condition *(page 158, new traces of behavior are collected, using the same method as for collecting a pattern of normal behavior)*.

As per claim 5, Hofmeyr teaches the method of claim 1 as applied above. Hofmeyr additionally teaches the method wherein comparing the pattern statistic to the prototype statistic further comprises comparing a frequency *(page 156, models of normal user behavior can be generated in terms of frequency distributions)* and a consequence *(page 153, sequences of system calls are used as a discriminator for determining intrusion)* associated with the pattern statistic to another frequency and another consequence associated with the prototype statistic.

As per claim 11, Hofmeyr teaches an apparatus encoded with computer-executable components for determining tamper evidence of a client process, comprising: a transceiver arranged to receive and forward data *(page 154, an intrusion detection system used to determine anomalous behavior, can be host-based or network-based. In the latter case, it is inherent that there be a transceiver within the system in order to communicate activity from a particular host)*; an interface, coupled to the transceiver, and arranged to perform actions, including: <u>determining a trait associated with the client process</u> *(page 152, system calls serve as the observable characteristic of a program)*; <u>receiving a first set of data associated with the trait based in part on execution of the client process in a normal condition</u> *(page 153, data is collected of normal behavior in a normal execution environment)*; <u>receiving a second set of data associated with the trait based in part on another execution of the client process in another condition</u> *(page 158, new traces of behavior are collected, using the same method as for collecting a pattern of normal behavior)*; <u>determining a pattern statistic associated with the first set of data</u> *(page 177, normal behavior is defined in terms of short sequences of system calls executed by running privileged processes; page 156, this data is used to build up profiles/databases of normal behavior)*; <u>determining a prototype statistic associated with the second set of data</u> *(page 158, the same method used to generate the normal behavior data is used to collect data at another instance)*; <u>comparing the pattern statistic to the prototype statistic</u> *(page 155, deviations from normal behavior may indicate possible intrusions. Hence, behavior at another instance is compared against normal behavior to determine any deviations.)*; <u>and if the comparison indicates abnormal behavior of the client process, performing a predetermined action</u> *(page 155, the IDS informs the system administrators of anomalous or intrusive behavior)*.

As per claim 12, Hofmeyr teaches the apparatus of claim 11 as applied above. Hofmeyr additionally teaches the apparatus wherein the computer-executable components reside in at least one of a server, and a client *(page 154, an intrusion detection system used to determine anomalous behavior, can be host-based or network-based. In the latter case, it the system being monitored can be considered the "client" which may report to a central machine where all processing is performed)*.

As per claim 15, Hofmeyr teaches the apparatus of claim 11 as applied above. Hofmeyr additionally teaches the apparatus wherein determining the pattern statistic and the prototype statistic further comprises: determining a trend associated with the trait during execution of the client process in the normal condition *(page 177, normal behavior is defined in terms of short sequences of system calls executed by running privileged processes)*; and determining another trend associated with the trait during the other execution of the client process in the other condition *(page 158, new traces of behavior are collected, using the same method as for collecting a pattern of normal behavior)*.

As per claim 20, Hofmeyr teaches a system for determining tamper evidence of a computing process, comprising: a client that includes the computing process, and is configured to communicate trait data associated with an execution of the computing process; and a server, coupled to the client, and arranged to perform actions *(page 154, an intrusion detection system used to determine anomalous behavior, can be host-based or network-based. In the latter case, it*

the system being monitored can be considered the "client" which may report to a central

machine where all processing is performed), including: receiving a first set of data associated

with the trait based in part on execution of the computing process in a normal condition *(page*

153, data is collected of normal behavior in a normal execution environment); receiving a

second set of data associated with the trait based in part on another execution of the computing

process in another condition *(page 158, new traces of behavior are collected, using the same*

method as for collecting a pattern of normal behavior); determining a pattern statistic associated

with the first set of data *(page 177, normal behavior is defined in terms of short sequences of*

system calls executed by running privileged processes; page 156, this data is used to build up

profiles/databases of normal behavior); determining a prototype statistic associated with the

second set of data *(page 158, the same method used to generate the normal behavior data is used*

to collect data at another instance); comparing the pattern statistic to the prototype statistic

(page 155, deviations from normal behavior may indicate possible intrusions. Hence, behavior

at another instance is compared against normal behavior to determine any deviations); and if the

comparison indicates abnormal behavior of the computing process, performing a predetermined

action *(page 155, the IDS informs the system administrators of anomalous or intrusive*

behavior).

        As per claim 21, Hofmeyr teaches the system of claim 20 as applied above. Hofmeyr

additionally teaches the system wherein comparing the pattern statistic to the prototype static

further comprises employing a graphical representation to compare the pattern statistic to the

prototype statistic *(Figures 2 and 3)*.

As per claim 22, Hofmeyr teaches an apparatus for verifying integrity of a computing process, comprising: <u>a means for determining a trait associated with the computing process</u> *(page 152, system calls serve as the observable characteristic of a program)*; <u>a means for determining a pattern statistic associated with the trait based in part on execution of the computing process in a normal condition</u> *(page 153, data is collected of normal behavior in a normal execution environment)*; <u>a means for determining a prototype statistic associated with the trait based in part on another execution of the computing process in another condition</u> *(page 158, new traces of behavior are collected, using the same method as for collecting a pattern of normal behavior)*; <u>a means for comparing the pattern statistic to the prototype statistic</u> *(page 155, deviations from normal behavior may indicate possible intrusions. Hence, behavior at another instance is compared against normal behavior to determine any deviations.)*, <u>and if the comparison indicates abnormal behavior, a means for performing a predetermined action</u> *(page 155, the IDS informs the system administrators of anomalous or intrusive behavior)*.

Allowable Subject Matter

5.   Claims 6-10 and 16-19 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See MPEP 707.05(c).

Detecting Intrusions Using System Calls: Alternative Data Models (Warrender, Forrest, & Pearlmutter, 1999)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to VIRGINIA HO whose telephone number is 571-270-7309. The examiner can normally be reached on Mon to Thu; 7:30 AM - 5:00 PM (Eastern).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/VIRGINIA HO/
Examiner, Art Unit 2432

/V. H./

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432